Hi --

In connection with

Enforceable mechanisms

The CPS workgroup understands that there may be one or more appropriate mechanisms to properly enforce and ensure that confidentiality, privacy, and security requirements are met in an electronic health information exchange environment. Therefore, the workgroup is interested in comments on appropriate, effective, and feasible ways to enforce confidentiality, privacy, and security protections in this new environment. Comments will be considered by the workgroup for the purposes of developing one or more recommendations associated with the "working hypothesis" above.

please consider some new security technology for databases.

The technology is called "Semantic Encoding". It is different from encryption, but complementary to it.

Whereas encryption is based on mathematical problems that are hard to solve, Semantic Encoding is based on a mathematical problem that is known to be unsolvable. Semantic Encoding also makes it impossible for an attacker to know whether or not he has succeeded, and tends to mislead a casual hacker towards a wrong decode. Very fast key changes are possible, without the need to re-encrypt a whole database. Different keys can be assigned to different, possibly overlapping parts of the data.

Please see www.reengineeringllc.com/semantic_encoding.html for full details.

Thanks, -- Adrian Walker

Internet Business Logic (R)
A Wiki for Executable Open Vocabulary English
Online at www.reengineeringllc.com Shared use is free

Adrian Walker
Reengineering

Ref: http://www.hhs.gov/healthit/ahic/confidentiality/cps_instruct.html